City of Fresno

125050

SYSTEMS SECURITY ADMINISTRATOR

DEFINITION

Under general direction, develops and implements data security systems that will provide detection, prevention, containment and deterrence mechanisms to protect and maintain the integrity of data files throughout the city.

SUPERVISION RECEIVED/EXERCISED

Receives general direction from the Information Services Manager.
Exercises supervision over Network Systems Staff.

DISTINGUISHING CHARACTERISTICS

The Systems Security Administrator develops and maintains policies and procedures that are designed to protect computer programs, databases and data files from unauthorized or accidental duplication, modification or destruction. Establishes and maintains correct access rules defining who has access to which data sets under what circumstances. This is a single class position which is distinguished from the next higher class of Information Services Manager in that incumbents of the latter assume responsibility for a division. It is distinguished from Senior Network Systems Specialist in that the incumbent of the latter has overall responsibility for the field of operations of the Network Systems Staff.

EXAMPLES OF IMPORTANT AND ESSENTIAL DUTIES

(May include, but are not limited to the following.)

Prevent unauthorized access to data and resources on the network. Design, implement, maintain and audit network and computer security policies. Determine areas of weakness in the security architecture. Monitor the network for security breaches. Specify and implement solutions for controlling weaknesses in the security architecture. Implement the policies and test their effectiveness in real-time scenarios. Document policies and procedures.

Responsible for the design, implementation and administration of virus scanner, firewalls and intrusion detection systems. Continually monitor hacking techniques and the hacking culture. Track down hackers when security breaches occur.

Educate staff and end users about network security, supporting skill levels ranging from novice to expert. Document detection intrusions and provide relevant information to internal and external security personnel. Update policies and procedures to prevent similar intrusions.

Manages disaster recovery functions for information systems, organizing off-site storage necessary for recovery processes, and overseeing development of recovery procedures. Disseminates and trains staff on security policies and practices as well as develops strategies and plans to provide for timely business resumption in the event a serious disruption; initiates, facilitates, and promotes activities to create information security awareness within the city.

Responsible for performing information security risk assessments on IT systems, identifying vulnerabilities and providing recommendations on mitigating or resolving vulnerabilities; makes recommendations for short and long-range security planning in response to city needs and new technology.

Maintain a broad understanding of issues regarding information security technologies, federal and state laws, industry best practices, exposures and related regulatory issues.

Performs general network administration, user support and other network functions as assigned.

Performs other related duties as assigned.

JOB-RELATED AND ESSENTIAL QUALIFICATIONS

Knowledge of:

Network and system security technology and practices including mainframe, client/server, PC/LAN, telephony and Internet related technology.

Current technology in operating systems, database administration, application development technologies, and industry trends. Understanding of backup infrastructures; compilation, configuration and system-level security procedures.

Database administration and the ability to effectively perform installations, configuration management, security, back-up and recovery procedures.

System design and analysis, client-server architecture, along with relevant technical knowledge of database systems.

Security such as Firewalls, Intrusion Detection Systems (IDS), and Network Sniffing Systems.

Skill to:

Operate an office computer and a variety of word processing and software applications.

Ability to:

Maintain the integrity and security of databases and information regarding customers, employees, and business information. Able to secure operation of all servers and services through the use of security and encryption tools.

Use independent judgment and initiative in making recommendations regarding information security, development and enforcement.

Develop programs and support systems and conduct system analysis and development to keep systems current with changing technologies.

Communicate clearly and concisely, both orally and in writing, and prepare clear and concise written reports and correspondence.

Establish and maintain positive working relationships with representatives of community organizations, state/local agencies and associations, City management and staff, and the public.

MINIMUM QUALIFICATIONS

Experience:

Four years of information systems security, networking or related experience, which included two years of lead or supervisory experience.

Education:

Graduation from an accredited college or university with a Bachelor's degree.

Special Requirement(s):

Possession of a valid California Class C driver's license may be required at time of appointment.

Bachelor's degree in Computer Science, Information Systems, Business Administration, or related field preferred.

CISSP (Certified Information Systems Security Professional), or CCSP (Cisco Certified Security Professional) certifications are preferred.

APPROVED:_____ DATE:_____
Director

NK:SLR:12/22/04
Revised 03/16/05